AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1-22 (canceled)

23. (New) A method of securely initializing subscriber and security data in a mobile routing system when the subscribers are also subscribers of a radio communication network, the method comprising:

re-running an authentication and key agreement procedure defined for the radio communication network, between a mobile node and an authentication server of the radio communication network;

providing a shared secret resulting from the re-running of the authentication and key agreement procedure to a stable forwarding agent of the mobile routing system, and using the shared secret to authenticate the mobile node to the stable forwarding agent;

agreeing upon keys by which further communications between the mobile node and the stable forwarding agent can be secured;

following authentication of the mobile node to the stable forwarding agent, collecting at the stable forwarding agent subscriber contact information from said authentication server; and

using the subscriber information and keys in providing mobility services to subscriber mobile nodes and correspondent nodes, including using the subscriber information to assign a Fully Qualified Domain Name and/or IP address to the mobile node.

24. (New) A method according to claim 23, further comprising:

transporting messages associated with the re-running step, between the stable forwarding agent used by a mobile node and the authentication server via the stable forwarding agent.

25. (New) A method according to claim 23, further comprising:

sending session keys, agreed upon during the re-run authentication procedure, from the authentication server to the stable forwarding agent.

26. (New) A method according to claim 23, further wherein the mobile routing system is a Mobile IP based system, and the stable forwarding agent is a Home Agent.

27. (New) A method according to claim 23, wherein the mobile routing system is a HIP based system.

28. (New) A method according to claim 23, wherein said authentication and key agreement procedure is the Authentication and Key Agreement procedure specified by 3GPP.

29. A method according to claim 23, wherein the collected subscriber information comprises one or more of the following:

the name and postal address of a subscriber;

the telephone number associated with a subscriber;

the existing Fully Qualified Domain Name for a subscriber; and the status of any mobility services established earlier for a subscriber.

30. (New) A stable forwarding agent of a mobile routing system, the stable forwarding agent comprising:

a relay for relaying messages associated with a re-run of an authentication and key agreement procedure between a mobile node and an authentication node of a radio communication network;

a receiver for receiving a shared secret from the authentication server following completion of the procedure for using the shared secret to authenticate the mobile node and for collecting subscriber contact information from the authentication server;

a key determining processor for agreeing upon keys by which further communications between the mobile node and the stable forwarding agent can be secured; and

a mobility service provisioning processor for using said subscriber information and keys in the provision of mobility services to subscriber mobile nodes including using the subscriber information to assign a suitable Fully Qualified Domain Name and/or IP address to said mobile node.